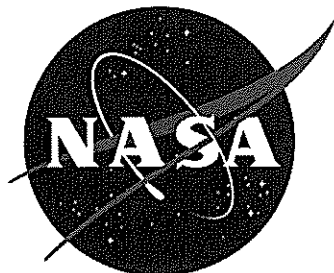


# NASA Information Technology Requirement



**NITR 2810-15**

Effective Date: June 9, 2008

Expiration Date: May 16, 2011

---

## Contingency Planning

---

Responsible Office: Office of the Chief Information Officer

## **PREFACE**

- P.1 PURPOSE
- P.2 APPLICABILITY
- P.3 AUTHORITY
- P.4 APPLICABLE DOCUMENTS
- P.5 MEASUREMENT AND VERIFICATION
- P.6 CANCELLATION

## **1.0 REQUIREMENT**

- 1.1 General
- 1.2 Contingency Planning Policy and Procedures (CP-1)
- 1.3 Contingency Plan (CP-2)
- 1.4 Contingency Training (CP-3)
- 1.5 Contingency Plan Testing and Exercises (CP-4)
- 1.6 Contingency Plan Update (CP-5)
- 1.7 Alternate Storage site (CP-6)
- 1.8 Alternate Processing site (CP-7)
- 1.9 Telecommunications Services (CP-8)
- 1.10 Information System Backup (CP-9)
- 1.11 Information System Recovery and Reconstitution (CP-10)

## **APPENDIX A. Definitions**

## **APPENDIX B. Acronyms**

### **Distribution:**

### **NODIS**

**Change History**

Change Number	Date	Change Description

## **PREFACE**

### **P.1 PURPOSE**

- a. This NASA Information Technology Requirement (NITR) describes the Agency procedural requirements and responsibilities for implementation of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 2, Contingency Planning family of security controls.
- b. This NITR is an addendum to NASA Procedural Requirements (NPR) 2810.1A, Security of Information Technology.

### **P.2 APPLICABILITY**

- a. This NITR applies to unclassified information systems at NASA Headquarters and Centers, including Component Facilities and Technical and Service Support Centers. To the extent specified in their respective contracts or agreements, it applies to the NASA Jet Propulsion Laboratory, other contractors, grant recipients, or parties to agreements for information systems that they use or operate on behalf of the Agency or that support the operations and assets of the Agency.

### **P.3 AUTHORITY**

- a. Reference Paragraph P.3, NPR 2810.1A

### **P.4 APPLICABLE DOCUMENTS**

- a. NPR 2810.1A, Security of Information Technology.
- b. NITR 2810-12, Continuous Monitoring.
- c. ITS-SOP-0040 Contingency Planning Guidance.
- d. NPR 1040.1, NASA Continuity of Operations (COOP) Planning Procedural Requirements.
- e. Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems
- f. NIST SP 800-100, Information Security Handbook: A Guide to Managers.
- g. NIST SP 800-53 (Revision 2), Recommended Security Controls for Federal Information Systems.
- h. NIST SP 800-53A, DRAFT Guide for Assessing the Security Controls in Federal Information Systems.
- i. NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems.

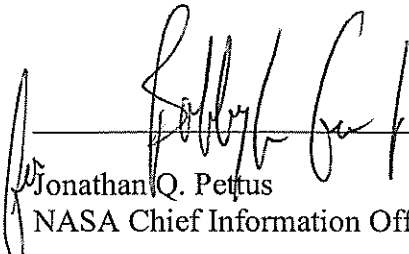
- j. NIST SP 800-30, Risk Management Guide for Information Technology Systems.
- k. NIST SP 800-84, Guide to Test, Training and Exercise Programs for IT Plans and Capabilities.
- l. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

#### **P.5 MEASUREMENT AND VERIFICATION**

- a. Meet the annual requirement to assess Contingency Planning family of security controls for all Agency information systems not later than July 31<sup>st</sup> of each year in accordance with this NITR, NITR 2810-12 Continuous Monitoring, and NIST SP 800-53 (Revision 2).
- b. Meet the annual requirement to conduct Contingency Plan test/exercise on all Agency information systems not later than July 31<sup>st</sup> of each year in accordance with this NITR and NIST SP 800-53 (Revision 2) Security Control CP-4, Contingency Plan Testing and Exercises.

#### **P.6 CANCELLATION**

- a. The next version of NPR 2810.1 cancels this NITR.

  
Jonathan Q. Pettus  
NASA Chief Information Officer

6/9/08  
Date

## **1.0 REQUIREMENT**

### **1.1 General**

Contingency planning shall provide for the establishment, maintenance, and effective implementation of plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

1.1.1 Contingency planning policy and procedures shall be consistent with all other NASA policies, applicable laws, directives, policies, standards, and guidance.

1.1.2 NASA Centers and Information System Owners (ISO) shall meet the contingency planning requirements of NIST 800-34 and NIST 800-53 (Revision 2) CP-2 through CP-10 Contingency Planning security controls for all information systems.

1.1.3 The ISO shall be responsible for contingency planning including the development, implementation, and maintenance of the CP-2 through CP-10 Contingency Planning security controls for all information systems for which they are responsible, in accordance with Agency contingency planning policy and procedures and ITS-SOP-0040 Contingency Planning Guidance.

1.1.4 The ISO shall ensure that CP-2 through CP-10 Contingency Planning security controls are assessed annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in accordance with NIST SP 800-37, paragraph 3.4, subtask 9.2 and results documented in RMS in accordance with NITR 2810-12 Continuous Monitoring.

### **1.2 Contingency Planning Policy and Procedures (CP-1)**

The Agency is responsible for developing, disseminating, and periodically reviewing/updating a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, compliance and procedures to facilitate the implementation of the contingency plan policy and associated contingency planning controls. The following policy addresses the requirement to develop and maintain an Agency contingency planning policy and procedures.

1.2.1 The CP-1 Contingency Planning Policy and Procedures security control applies to all FIPS-199 security categories.

1.2.2 Center Chief Information Officers (CIO) shall ensure implementation of Agency contingency planning policy and procedures to provide for emergency response, backup operations, and post-disaster recovery for Center information systems.

1.2.3 The Senior Agency Information Security Officer (SAISO) shall:

a. Annually review and update as necessary the CP-1 Contingency Planning Policy and

Procedures security control as an Agency common control.

- b. Annually obtain certification of the CP-1 security control as an Agency common control by an independent Certification Agent (CA).
- c. Ensure the certified CP-1 security control is documented as an Agency common control in the RMS C&A Documentation Repository and POA&M Management System, referred to as RMS.
- d. Review and update Contingency Planning policy and procedures as required to meet changes to NIST guidance or the Office of Management and Budget (OMB) directives.

### **1.3 Contingency Plan (CP-2)**

Contingency plans are a control that provides ISOs a mechanism to ensure the availability of information systems to prevent an impact to business functions in the event of emergency. The following policy addresses the requirement to develop and maintain contingency plans and business impact assessments for NASA information systems.

1.3.1 The information system Contingency Plan shall be reviewed and approved by the ISO, the Information System Security Officer (ISSO) that is assigned as principal advisor to that ISO, and the Center Information Technology Security Manager (ITSM).

1.3.1.1 The Center ITSM may designate the authority for review and approval of the contingency plans of Center information systems to an ITSM Designated Representative.

1.3.1.1.1 The Center ITSM designated representative shall:

- a. Be in writing, identify specific delegated authority, and be signed by the Center ITSM.
- b. For FIPS-199 moderate and high-impact information systems, not be the ISSO that is assigned as principal advisor to the ISO.

1.3.2 The Information System Owners (ISO) shall:

- a. Appoint in writing the Contingency Plan Coordinator (CPC) for individual information system(s)
- b. For all information systems for which they have responsibility, develop contingency plans, including a business impact assessment, in accordance with ITS-SOP-0040 Contingency Planning Guidance, NIST SP 800-34 Contingency Planning Guide for Information Technology Systems and NPR 1040.1 NASA Continuity of Operations (COOP) Planning Procedural Requirements.
- c. For FIPS-199 moderate and high-impact information systems, coordinate development of contingency plans with other organizational elements responsible for related plans such as Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan and Emergency Action Plan.

- d. For FIPS-199 high-impact information systems, conduct capacity planning to identify the necessary capacity needed and available for information processing, telecommunications, and environmental support during crisis situations.
- e. For the contingency plan of an information system designated as Agency Mission Essential Infrastructure (MEI), at a minimum, develop and implement a contingency plan with the same requirements as for a FIPS-199 high-impact information system.
- f. For an information system that is a part of an Agency MEI, ensure that the contingency plan supports the MEI Continuity of Operations Plan (COOP) for mission essential operations and functions.
- g. Distribute signed copies of the contingency plan to key contingency personnel who are required for the plan implementation, decisions, support, and/or are impacted by the contingency plan.
- h. Ensure that a completed and signed copy of the information system Contingency Plan is included as part of the certification package in RMS.

1.3.3 The Authorizing Official (AO) may designate a CPC for specific individual or multiple systems for which they have AO responsibility.

1.3.3.1 The AO designation of the CPC shall be in writing.

#### **1.4 Contingency Training (CP-3)**

Personnel involved in the execution of an information system contingency plan need to be trained on their responsibilities to prepare them for participation in exercises, tests, and actual emergency situations related to that plan. The following policy addresses the requirement for all personnel involved in information system contingency planning to receive training on their roles and responsibilities in compliance with NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, NIST 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities and ITS-SOP-0040 Contingency Planning Guidance.

1.4.1 The ISO shall:

- a. Provide initial contingency plan training for all personnel involved in the execution of the information system contingency plan.
- b. Ensure training sessions precede exercises and tests so that personnel are familiar with their roles and responsibilities within a given contingency plan before exercising the plan itself.
- c. Provide refresher training annually, focusing on any changes implemented in the previous year or in areas where additional training is identified.
- d. Maintain contingency planning training records.
- e. Document completion of annual refresher training in RMS.



1.4.2 For FIPS-199 high-impact information systems, include simulated events in the training.

## 1.5 Contingency Plan Testing and Exercises (CP-4)

Executing contingency plans during controlled tests and/or exercises provides a mechanism to test the effectiveness of the contingency plans, the training provided and correct weaknesses in the plan in a controlled situation. The following policy addresses the requirement to conduct testing of contingency plans for Agency information systems on a regular basis.

1.5.1 There are several methods for testing and/or exercising contingency plans to identify potential weaknesses. The test types and procedures including objectives and scope are included in ITS-SOP-0040 Contingency Planning Guidance.

1.5.2 The depth and rigor of contingency plan testing and/or exercises increases with the FIPS 199 impact level of the information system. The following contingency plan test strategy shall be used for contingency plan testing of Agency information systems:

System Category	Year 1 – Test Type	Year 2 – Test Type	Year 3 – Test Type
<b>Low</b>	Classroom Exercises/Tabletop Written Test	Classroom Exercises/Tabletop Written Test	Classroom Exercises/Tabletop Written Test  Integrated Test
<b>Moderate</b>	Classroom Exercises/Tabletop Test	Classroom Exercises/Tabletop Test with Scenarios	Functional Exercises/Simulation Exercise  Integrated Test
<b>High</b>	Functional Exercises/Simulation Exercise	Functional Exercises/Simulation Exercise	Functional Exercises/Alternate Site Test  Integrated Test

1.5.3 Center ITSMs shall ensure that contingency plans are tested/exercised annually for all Center information systems.

1.5.4 The ISO shall:

- a. Test/exercise information system contingency plans at least annually at approximately the same time each fiscal year, but completed no later than July 31<sup>st</sup> in compliance with NIST SP

800-34 Contingency Planning Guide for Information Technology Systems, NIST 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities and ITS-SOP-0040 Contingency Planning Guidance.

- b. Ensure the above Agency contingency plan test strategy is used to determine the type of contingency plan test/exercise to be conducted.
- c. Ensure that the contingency plan test/exercise is coordinated with organizational elements responsible for related plans such as Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan and Emergency Action Plan.
- d. For FIPS-199 high-impact information systems, test/exercise the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.
- e. Document completion of the annual contingency plan test/exercise in RMS.

## **1.6 Contingency Plan Update (CP-5)**

Contingency plans must be reviewed and updated on a regular basis as there are changes in information system components, changes in the organization and problems encountered during plan implementation, execution, or testing. The following policy addresses the requirement to review and update contingency plans for Agency information systems on a regular basis.

### **1.6.1 The ISO shall:**

- a. Annually review the contingency plan and update as necessary, communicating any change to individual and/or organization impacted by the change in accordance with NIST 800-34 Contingency Planning Guide for Information Technology Systems and ITS-SOP-0040 Contingency Planning Guidance.
- b. Provide a copy of the revised contingency plan to key contingency personnel.
- c. Update the information system certification package in RMS to include the updated contingency plan.
- d. Document completion of the contingency plan annual review in RMS.

1.6.2. The updated contingency plan shall be reviewed and approved by the ISO, the ISSO that is assigned as principle advisor to that ISO, and the Center ITSM.

## **1.7 Alternate Storage Site (CP-6)**

In order to support events requiring the recovery of information systems, the information system backups to recover the system must be stored at an alternate site. The following policy addresses the requirement to identify alternate sites for storage of information system backups.

1.7.1 For FIPS-199 moderate and high-impact information systems, the ISO shall:

- a. Provide an alternate storage site geographically separated from the primary storage site.
- b. Initiate the necessary agreements for storage of backup information system.
- c. Identify potential accessibility problems in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

1.7.2 For FIPS-199 high-impact information systems, the ISO shall ensure the alternate storage site is configured to facilitate timely and effective recovery operations.

1.7.3. The Center ITSM shall provide information system security expertise and support to the ISO for alternate site selection and acceptability.

## **1.8 Alternate Processing Site (CP-7)**

In order to support the recovery of information systems in an emergency, it may be necessary to recover at an alternate processing site in the event the primary site is not accessible. The following policy addresses the requirement to identify alternate sites for the resumption of information system operations in the event of a disaster or major disruption of services.

1.8.1 The AO shall ensure that resources are available to provide and provision the alternate processing site.

1.8.2 For FIPS-199 moderate or high-impact information systems, the ISO shall:

- a. Identify an alternate processing site geographically separated from the primary processing site.
- b. Initiate the necessary agreements to permit the resumption of information system operations for critical mission/business functions within the time specified in the information system contingency plan when the primary processing capabilities are unavailable.
- c. Ensure that the equipment and supplies required to resume operations are either available at the alternate site or contracts are in place to support delivery to the site.
- d. Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.
- e. Ensure the alternate processing site agreement contains priority-of-service provisions in accordance with availability requirements.

1.8.3 For FIPS-199 high-impact information systems, the ISO shall ensure the alternate processing site is configured so that it is ready to be used as the operational site supporting a minimum required operational capability.

## **1.9 Telecommunications Services (CP-8)**

Telecommunications services are a key in technology operations as such the organization needs to identify both the primary and alternate services that will support the IT operations. The following policy addresses the requirement to identify alternate telecommunications services for the resumption of information system operations in the event of a disaster or major disruption of services.

1.9.1 For FIPS-199 moderate and high-impact information systems, the ISO shall:

- a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements.
- b. Obtain alternate telecommunications services that do not share a single point of failure with primary telecommunications services.

1.9.2 For FIPS-199 high-impact information systems, the ISO shall:

- a. Obtain alternate telecommunications service providers that are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.
- b. Require primary and alternate telecommunications service providers to have adequate contingency plans.

## **1.10 Information System Backup (CP-9)**

In order to successfully recover an information system, the components of the system and data must be backed up successfully. For each information system it must be determined what required information is to be backed up for the successful recovery of the system. The following policy addresses the requirement to conduct backups of system-level and user-level information contained in Agency information systems.

1.10.1 The AO shall ensure that resources are provided to implement the information system backup requirements.

1.10.2 The ISO shall:

- a. Ensure that a backup strategy is established and implemented consistent with the recovery objectives stated in the information system contingency plan.
- b. Ensure that the backups include user-level and system-level information (including system state information) contained in the information system.
- c. At a minimum, test backup information annually during contingency plan testing to verify media reliability and information integrity.

d. Protect system backup information from unauthorized modification whenever it is removed from an Agency facility.

1.10.3 For FIPS-199 high-impact information systems, the ISO shall:

a. Ensure that backup copies of the operating system and other critical information systems software are stored in a fire-rated container that (1) is not collocated with the operational software or (2) is in a separate facility.

b. Selectively use backup information in the restoration of information system functions as part of the annual contingency plan test/exercise.

1.10.4. The Center ITSM shall:

a. Provide information system security expertise and support to the ISO and AO for the resourcing and implementation of information system backup requirements.

b. Provide security oversight of the implementation of backup requirements for Center information systems.

## **1.11 Information System Recovery and Reconstitution (CP-10)**

The goal of contingency planning is the successful recovery and reconstitution of the information system to a secure and usable state. The following policy addresses the requirement to implement mechanisms and procedures for the recovery of an information system after a disruption.

1.11.1 The ISO shall ensure mechanisms and procedures are available to allow the information system to be recovered and reconstituted to a known state after a disruption or failure.

1.11.2 For FIPS-199 high-impact information systems, the ISO shall ensure that there is a full recovery and reconstitution of the information system as part of the annual contingency plan test/exercise.

## Appendix A. Definitions

Term	Definition
Authorizing Official	An Agency official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals.
Authorizing Official Designated Representative	Individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.
Certification	<p>A formal process for testing components or systems against a specified set of security requirements. Certification is normally performed by an independent reviewer, rather than one involved in building the system. Certification is more often cost-effective for complex or high-risk systems. Less formal security testing can be used for lower-risk systems. Certification can be performed at many stages of the system design and implementation process and can take place in a laboratory, operating environment, or both.</p> <p>It provides a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.</p>
Chief Information Officer	Official responsible for: (1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, and regulations, and the priorities established by the head of the agency; (2) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (3) promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Term	Definition
Contingency Plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. Contingency plans assist managers to ensure that data owners continue to process (with or without computers) mission-critical applications in the event that computer support is interrupted.
Continuity of Operations Plan	Type of contingency related plan that provides procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days
Information Owner	An Agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information System	Discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems are also referred to as IT systems.
Information System Owner	An Agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. Responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the security requirements.
Information System Security Officer	The principal staff advisor to the information system owner on all matters involving the IT security of the information system. This responsibility may also include physical security, personnel security, incident handling, and security training and education. For smaller systems, a system administrator may perform the ISSO role as well as the system administrator role.
Mission Essential Infrastructure (MEI)	Critical infrastructures, physical, Cyber-based systems, or a combination, whose diminished capabilities would significantly impact the Federal Government's ability to perform essential national security missions and to ensure the general public health and safety; state and local governments to maintain order and to deliver minimum essential public services; and the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. (Reference Presidential Decision Directive (PDD) 63, May 22, 1998.)

Term	Definition
Plan of Action and Milestones	The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. POA&Ms are used to close security performance gaps, assist the Inspector General (IG) in their evaluation work of agency security performance, and assist OMB with oversight responsibilities.
RMS C&A Documentation Repository and POA&M Management System	A SecureInfo Corporation application used as the Agency's enterprise tool to document and track all Agency information system certification and accreditation, security control assessments and both system and programmatic vulnerabilities and weaknesses.
Senior Agency Information Security Official (SAISO)	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the Agency's Authorizing Officials, Information System Owners, and Information System Security Officers.
System	See Information System
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.



## **Appendix B. Acronyms**

AO	Authorizing Official
AODR	Authorizing Official Designated Representative
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
CPC	Contingency Plan Coordinator
FISMA	Federal Information Security Management Act
ISO	Information System Owner
ISSO	Information System Security Officer
ITSM	Information Technology Security Manager
MEI	Mission Essential Infrastructure
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NODIS	NASA Online Directives Information System
NPR	NASA Procedures and Requirements
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
POA&M	Plan of Actions and Milestones
RMS	RMS C&A Documentation Repository and POA&M Management System
SAISO	Senior Agency Information Security Officer
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plan